CMMC 2.0 CYBERSECURITY COMPLIANCE FOR DOD CONTRACTS

Security & Compliance: Now & Tomorrow

Any Framework, Any Time, Any Place

H&V Facility Solutions, Inc.

FLORIDA SURETY BONDS, INC.

Introductions & Welcome

Overview of CMMC 2.0

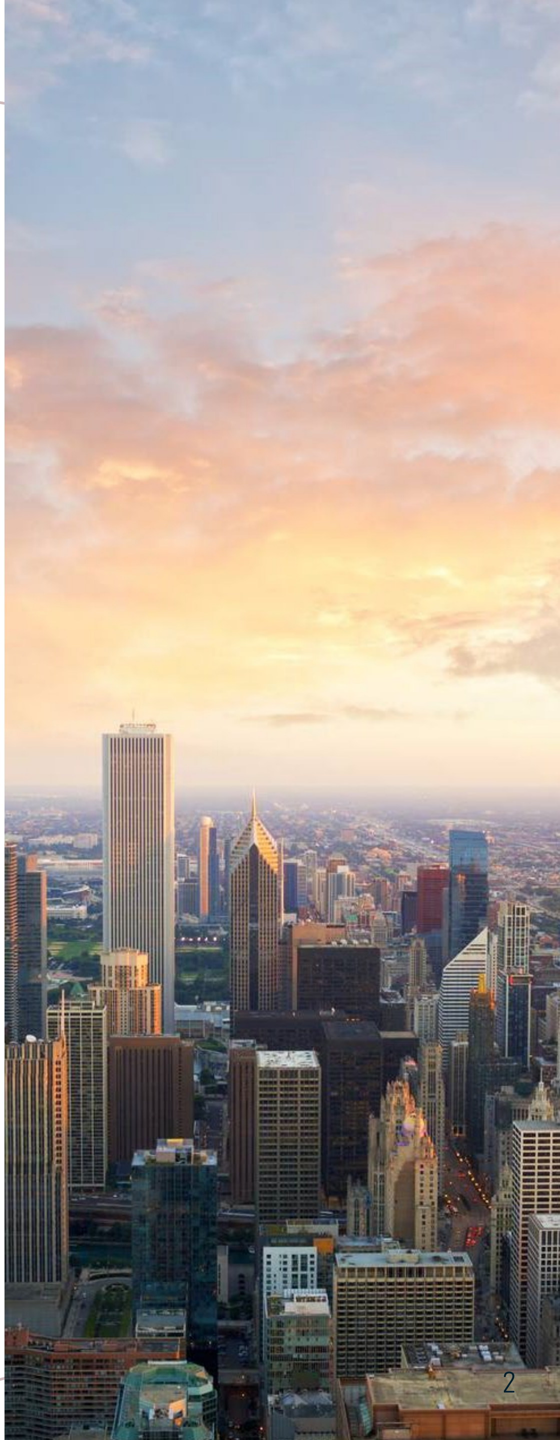
Implementation

Practical Considerations for DoD Contractors

Steps to Maintain Compliance in 2025

Latest News and Developments from CyberAB.org

Q&A



INTRODUCTION & WELCOME

- Vice President at H&V Facility Solutions, a Woman-Owned Small Business founded in 2022
- Been in the Mechanical Construction space since 2016 specializing in Building Automation, HVAC, Plumbing, and low voltage systems.
- Chemical Engineering & Music Studies degree from USF
- Career Focus on leveraging cutting edge tools and techniques to make traditional industries operate faster, better, easier, and recently – with easier compliance

WHY CMMC 2.0 MATTERS FOR AMERICA

SENIOR PENTAGON OFFICIAL SAYS CYBER WARFARE POSES SIGNIFICANT THREAT TO JOINT FORCE – JOHN GARSTKA

THE THREAT IS REAL- CYBER EXPO 2025

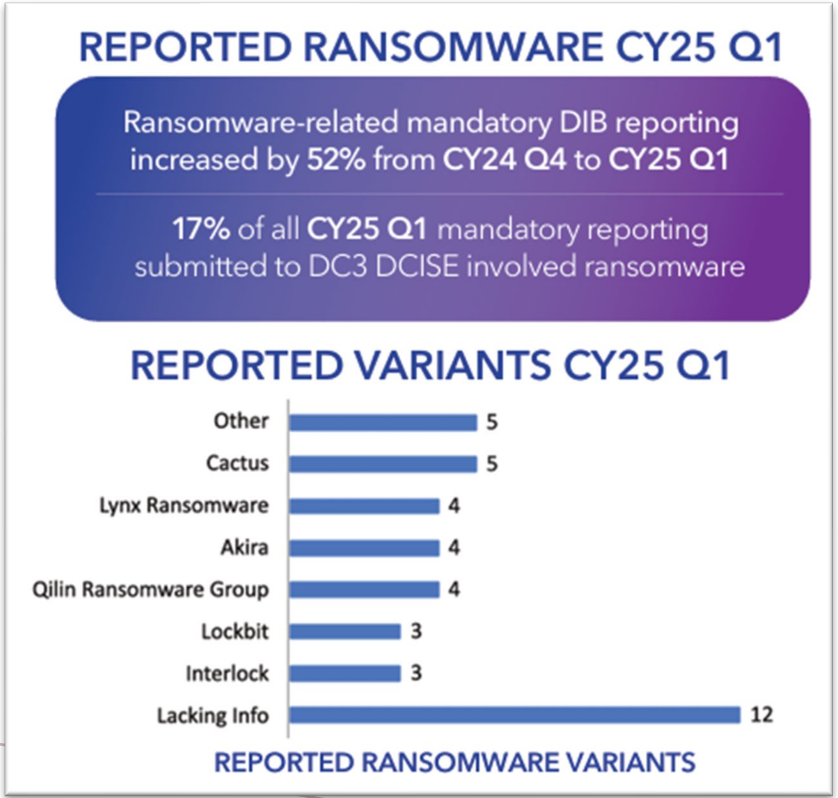
"What we have learned [from our wargaming] is that this is a significant threat that we have to prepare the joint force to deal with,"

Regarding which systems are most at risk of cyberattack, Garstka said America's adversaries — including China — often focus on the defense industrial base.

"We're not talking about hypotheticals here. If you're dependent on the DIB for operations of your space systems, you have to treat protecting the DIB as important as protecting the space system, space segment or ground segment,"

GOALS OF CMMC (CYBERSECURITY MATURITY MODEL) 2.0

THE CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS) DOCUMENTED 6 SIGNIFICANT CYBER INCIDENTS IN 2025 (UP TO SEPTEMBER) WITH DIRECT OR INDIRECT TIES TO THE U.S. DIB OR ALLIED DEFENSE SECTORS, INCLUDING:



REPORTED RANSOMWARE CY25 Q1

Ransomware-related mandatory DIB reporting increased by **52%** from **CY24 Q4** to **CY25 Q1**

17% of all **CY25 Q1** mandatory reporting submitted to DC3 DCISE involved ransomware

REPORTED VARIANTS CY25 Q1

Variant	Count
Other	5
Cactus	5
Lynx Ransomware	4
Akira	4
Qilin Ransomware Group	4
Lockbit	3
Interlock	3
Lacking Info	12

REPORTED RANSOMWARE VARIANTS

DoD Cyber Crime DIB-Reported Cyber Threats

January: Russian surge in Ukraine Attacks affecting US DIB aid (4,315 incidents in 2024)

February: Chinese Origin attacks (1,300+ in 2024)

March: Chinese-Linked front recruiting ex- U.S. Federal Workers

April: Chinese Malware on Latin American networks impacting U.S. Defense

May: Russian Campaign targeting NATO defense Supply Chains

OVERVIEW OF CMMC 2.0

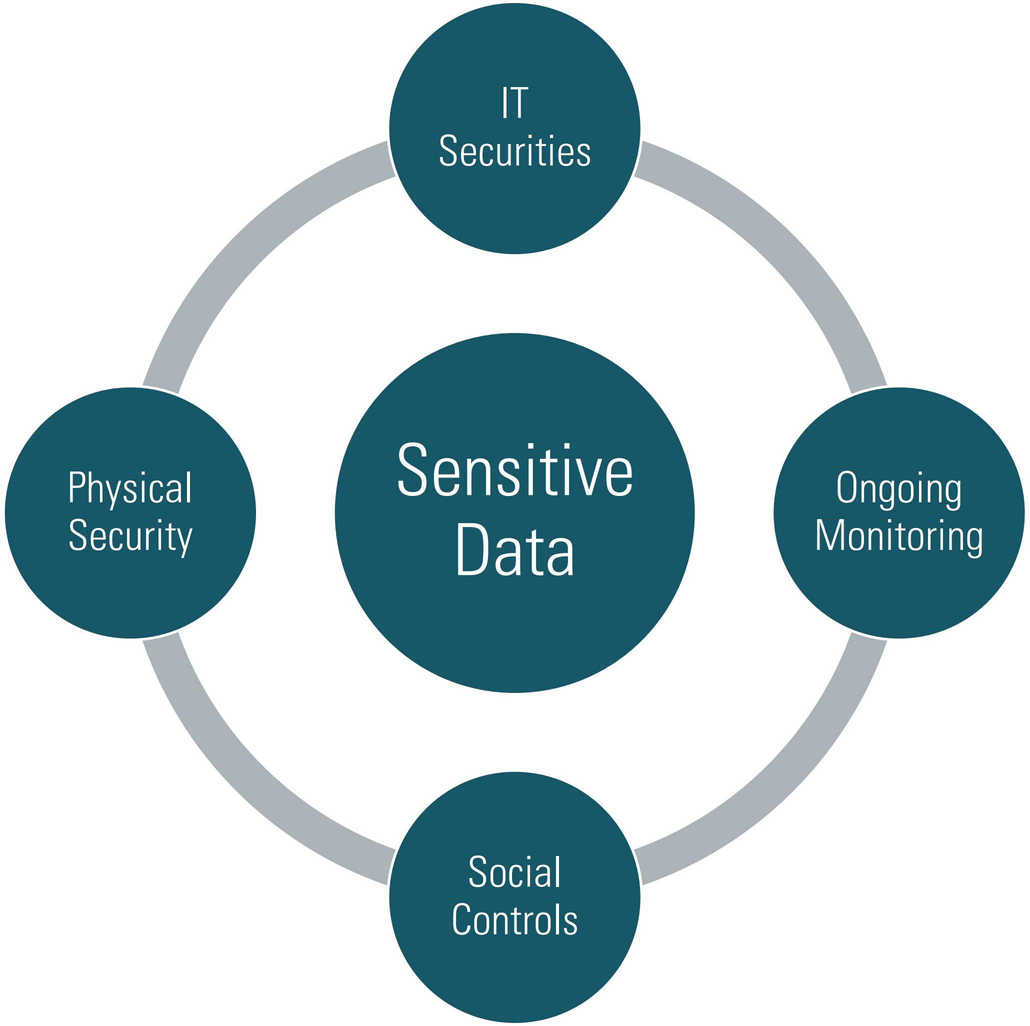
WHAT IS CMMC 2.0?

CMMC 2.0 is a framework to protect defense information relevant to adversaries and our Industrial Base:

- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)

CMMC Domains per DoD CIO CMMC v 2.13

- Access Controls (AC)
- Awareness & Training (AT)
- Audit & Accountability (AU)
- Configuration Management (CM)
- Identification & Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Risk Assessment (RA)
- Security Assessment (CA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)



How large do I have to build my defenses?

CORE FRAMEWORK & LEVELS

LEVEL	CONTROL COUNT	ASSESSMENT TYPE	ALIGNMENT WITH NIST
1	15	Self	FAR 52.204-21
2	110	Self or 3rd Party	NIST SP 800-171 Rev 2
3	110+24	Government	NIST SP 800-171 Rev 2 + SP 800-172

Requires Audit, Remediation, then C3PAO Certifier

IMPLEMENTATION

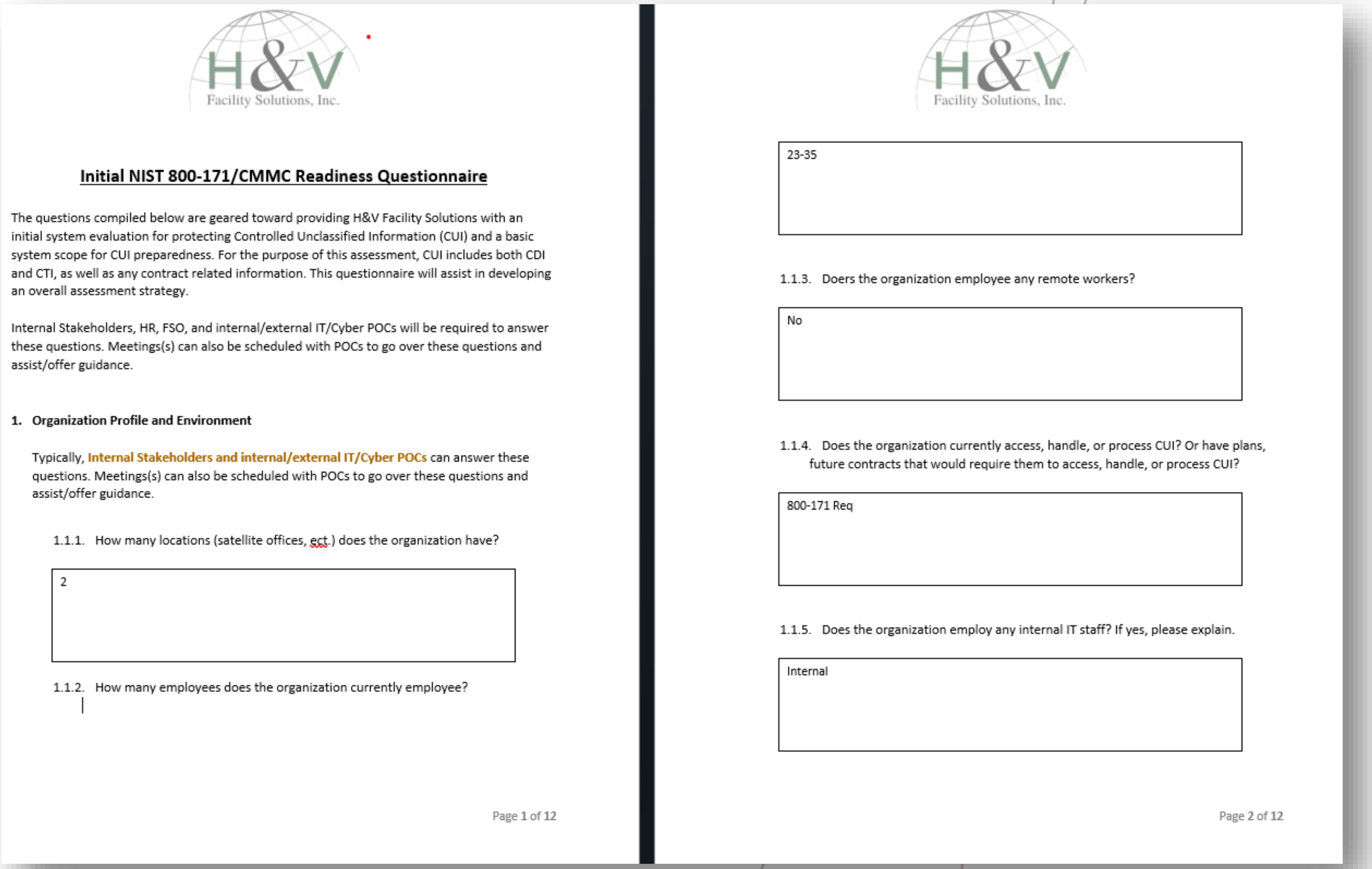
5 STEPS TO CMMC 2.0 COMPLIANCE

	Strategy & Program Management	Assessment & Gap Analysis	Remediation & Documentation	3rd Party Assessment	Monitoring & Reporting
Manual	1 month	1.5 months	13 months	3 months	Continuous
Automated	2 weeks	2 weeks	6 months	1 month	
	50% Savings	66% Savings	54% Faster	25% Faster	50% Savings

STRATEGY & PROGRAM MANAGEMENT

Initial Readiness Questionnaire

1. Organization Profile & Environment
2. Access Control/Audit – Internal IT or External MSP (technical)
3. Personal Security / Awareness & Training
4. Physical Protection
5. Risk-Security Assessment/Incident Response
6. System & Information Integrity/Maintenance



H&V Facility Solutions, Inc.

Initial NIST 800-171/CMMC Readiness Questionnaire

The questions compiled below are geared toward providing H&V Facility Solutions with an initial system evaluation for protecting Controlled Unclassified Information (CUI) and a basic system scope for CUI preparedness. For the purpose of this assessment, CUI includes both CDI and CTI, as well as any contract related information. This questionnaire will assist in developing an overall assessment strategy.

Internal Stakeholders, HR, FSO, and internal/external IT/Cyber POCs will be required to answer these questions. Meetings(s) can also be scheduled with POCs to go over these questions and assist/offer guidance.

1. Organization Profile and Environment

Typically, **Internal Stakeholders and internal/external IT/Cyber POCs** can answer these questions. Meetings(s) can also be scheduled with POCs to go over these questions and assist/offer guidance.

1.1.1. How many locations (satellite offices, ect.) does the organization have?

2

1.1.2. How many employees does the organization currently employee?

Page 1 of 12

H&V Facility Solutions, Inc.

23-35

1.1.3. Doers the organization employee any remote workers?

No

1.1.4. Does the organization currently access, handle, or process CUI? Or have plans, future contracts that would require them to access, handle, or process CUI?

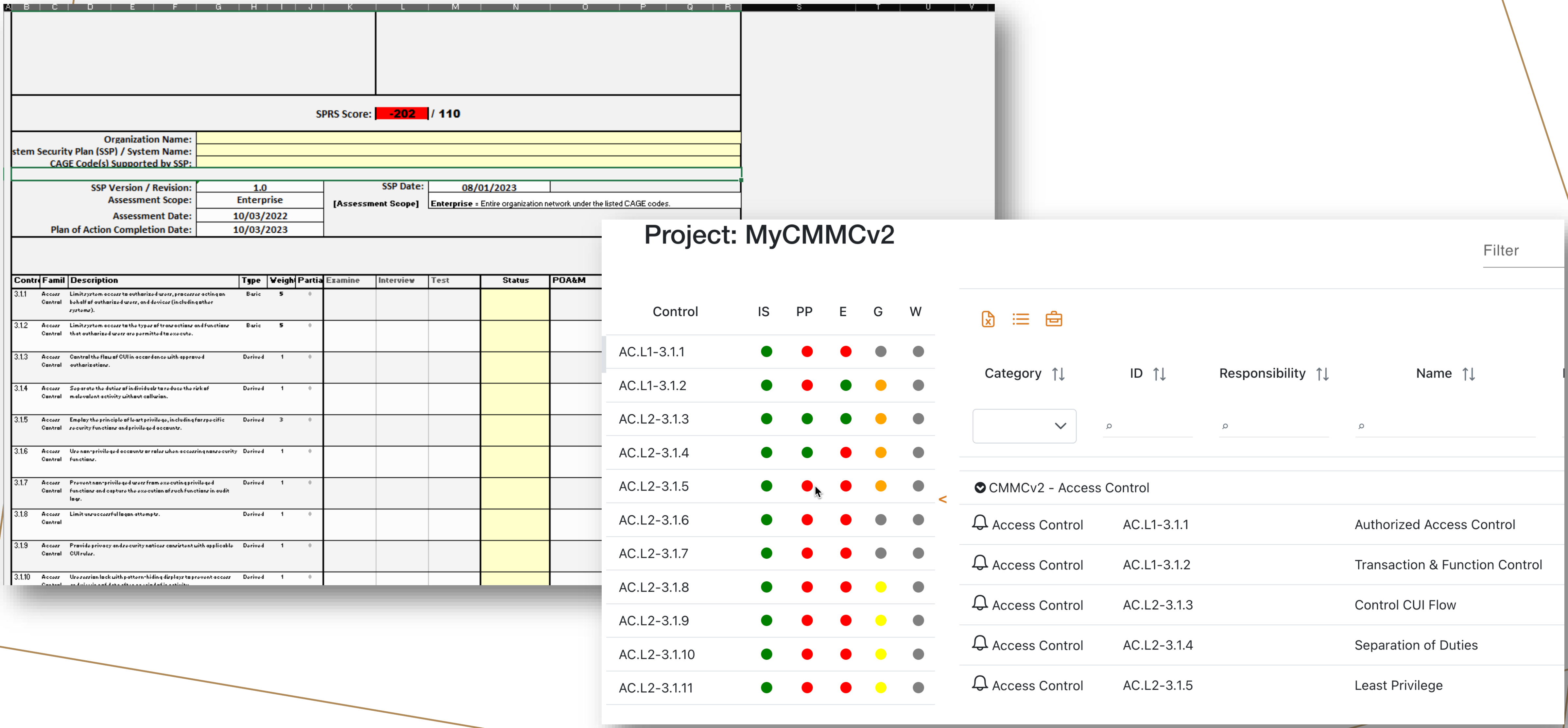
800-171 Req

1.1.5. Does the organization employ any internal IT staff? If yes, please explain.

Internal

Page 2 of 12

ASSESSMENT & GAP ANALYSIS



SPRS Score: -202 / 110

Organization Name:	
stem Security Plan (SSP) / System Name:	
CAGE Code(s) Supported by SSP:	

SSP Version / Revision:	1.0	SSP Date:	08/01/2023
Assessment Scope:	Enterprise	[Assessment Scope]	Enterprise = Entire organization network under the listed CAGE codes.
Assessment Date:	10/03/2022		
Plan of Action Completion Date:	10/03/2023		

Contr	Famil	Description	Type	Weigh	Partia	Examine	Interview	Test	Status	POA&M
3.1.1	Access Control	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Basic	5	0					
3.1.2	Access Control	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Basic	5	0					
3.1.3	Access Control	Control the flow of CUI in accordance with approved authorizations.	Derived	1	0					
3.1.4	Access Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Derived	1	0					
3.1.5	Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Derived	3	0					
3.1.6	Access Control	Use non-privileged accounts or roles when accessing nonsecurity functions.	Derived	1	0					
3.1.7	Access Control	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Derived	1	0					
3.1.8	Access Control	Limit unsuccessful logon attempts.	Derived	1	0					
3.1.9	Access Control	Provide privacy and security notices consistent with applicable CUI rules.	Derived	1	0					
3.1.10	Access	Use session lock with pattern-hiding displays to prevent access	Derived	1	0					

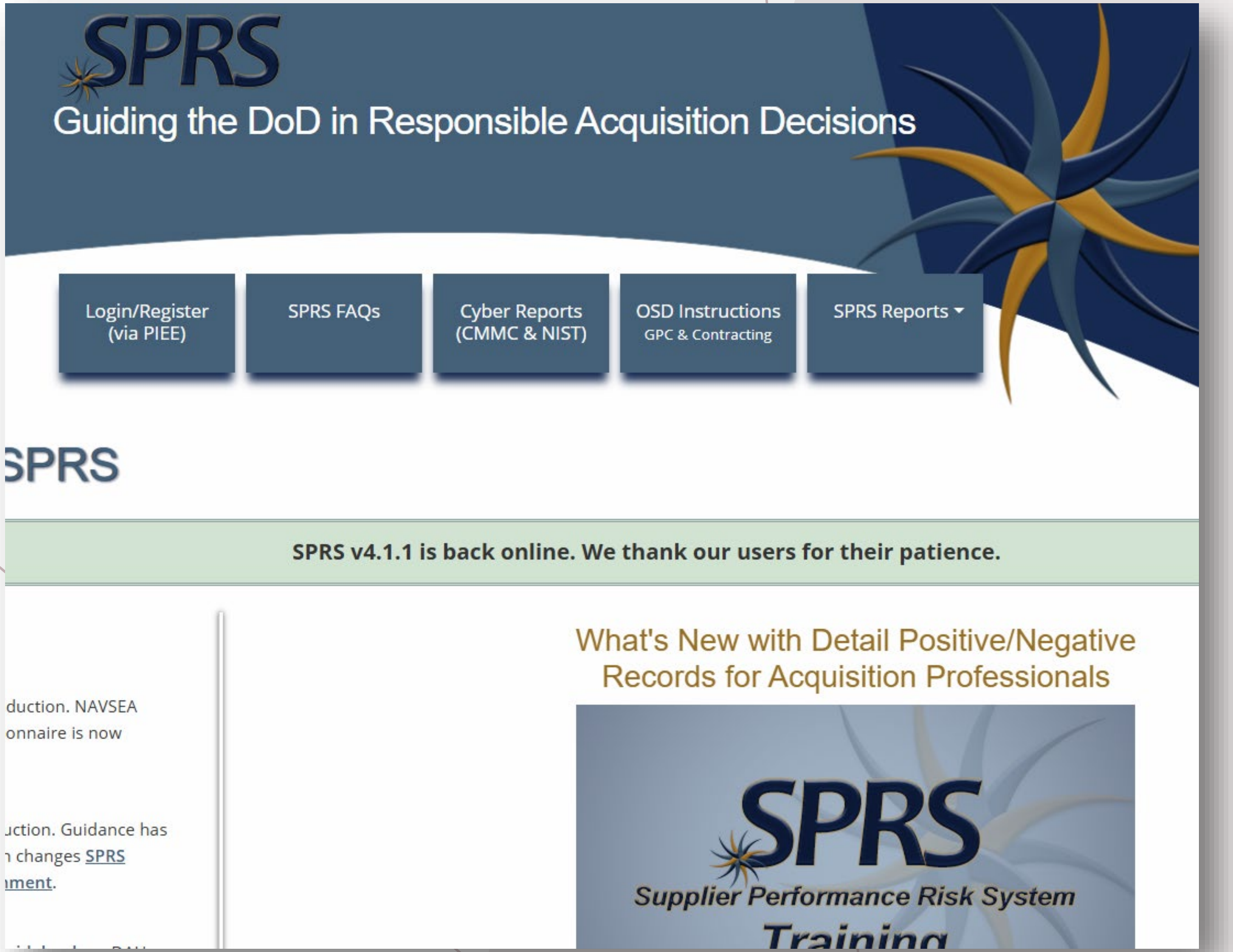
Project: MyCMMCv2

Filter

Control	IS	PP	E	G	W
AC.L1-3.1.1	🟢	🔴	🔴	⚪	⚪
AC.L1-3.1.2	🟢	🔴	🟢	🟠	⚪
AC.L2-3.1.3	🟢	🟢	🟢	🟠	⚪
AC.L2-3.1.4	🟢	🟢	🔴	🟠	⚪
AC.L2-3.1.5	🟢	🔴	🔴	🟠	⚪
AC.L2-3.1.6	🟢	🔴	🔴	⚪	⚪
AC.L2-3.1.7	🟢	🔴	🔴	⚪	⚪
AC.L2-3.1.8	🟢	🔴	🔴	🟡	⚪
AC.L2-3.1.9	🟢	🔴	🔴	🟡	⚪
AC.L2-3.1.10	🟢	🔴	🔴	🟡	⚪
AC.L2-3.1.11	🟢	🔴	🔴	🟡	⚪

CMMCv2 - Access Control

Category	ID	Responsibility	Name
Access Control	AC.L1-3.1.1		Authorized Access Control
Access Control	AC.L1-3.1.2		Transaction & Function Control
Access Control	AC.L2-3.1.3		Control CUI Flow
Access Control	AC.L2-3.1.4		Separation of Duties
Access Control	AC.L2-3.1.5		Least Privilege


SPRS
Login/Register (via PIEE)
SPRS FAQs
Cyber Reports (CMMC & NIST)
OSD Instructions GPC & Contracting
SPRS Reports
SPRS
Supplier Performance Risk System
Training

Guiding the DoD in Responsible Acquisition Decisions

SPRS

SPRS v4.1.1 is back online. We thank our users for their patience.

duction. NAVSEA
onnaire is now

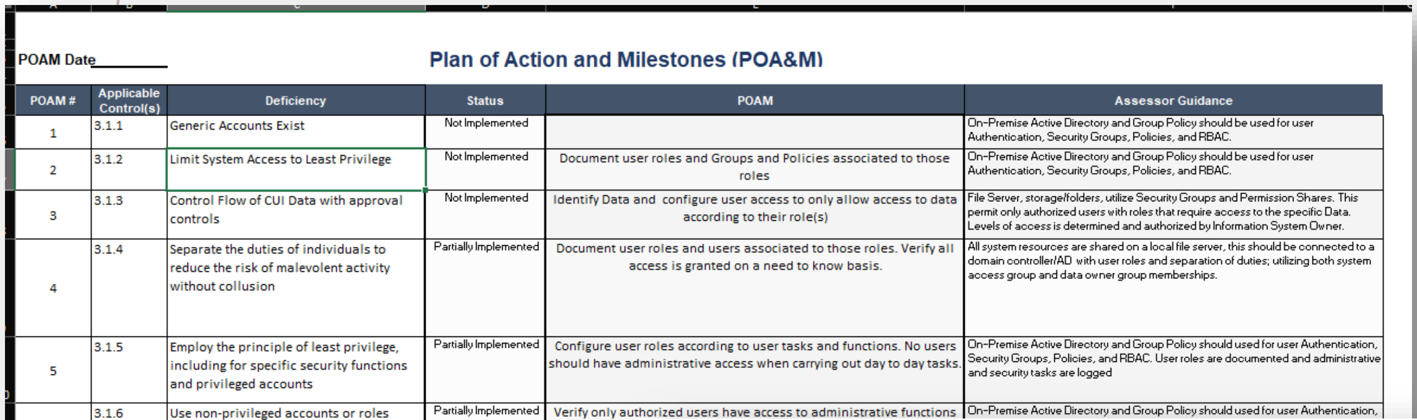
uction. Guidance has
n changes SPRS
ment.

What's New with Detail Positive/Negative Records for Acquisition Professionals

SPRS – SUPPLIER PERFORMANCE RISK SYSTEM

Supplier Performance Risk System

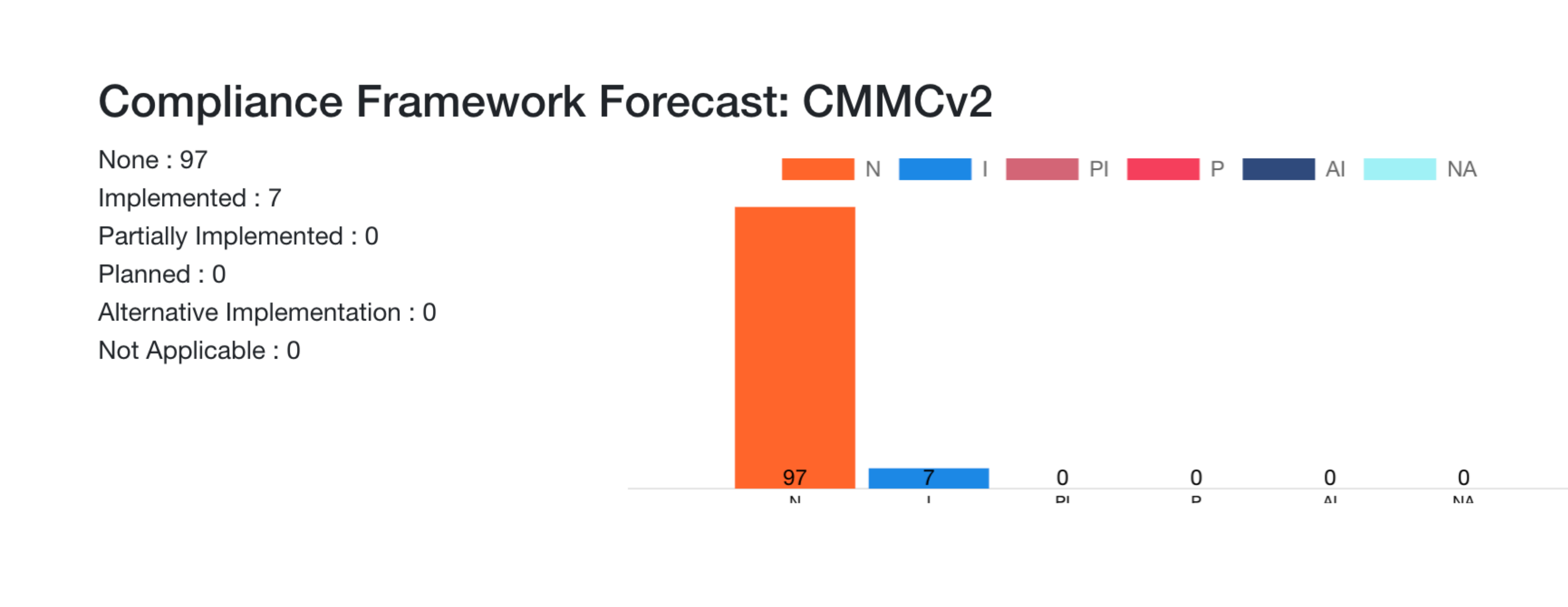
REMEDIATION & DOCUMENTATION



POAM Date__________

Plan of Action and Milestones (POA&M)

POAM #	Applicable Control(s)	Deficiency	Status	POAM	Assessor Guidance
1	3.1.1	Generic Accounts Exist	Not Implemented		On-Premise Active Directory and Group Policy should be used for user Authentication, Security Groups, Policies, and RBAC.
2	3.1.2	Limit System Access to Least Privilege	Not Implemented	Document user roles and Groups and Policies associated to those roles	On-Premise Active Directory and Group Policy should be used for user Authentication, Security Groups, Policies, and RBAC.
3	3.1.3	Control Flow of CUI Data with approval controls	Not Implemented	Identify Data and configure user access to only allow access to data according to their role(s)	File Server, storage/folders, utilize Security Groups and Permission Shares. This permit only authorized users with roles that require access to the specific Data. Levels of access is determined and authorized by Information System Owner.
4	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion	Partially Implemented	Document user roles and users associated to those roles. Verify all access is granted on a need to know basis.	All system resources are shared on a local file server, this should be connected to a domain controller/AD with user roles and separation of duties; utilizing both system access group and data owner group memberships.
5	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts	Partially Implemented	Configure user roles according to user tasks and functions. No users should have administrative access when carrying out day to day tasks.	On-Premise Active Directory and Group Policy should used for user Authentication, Security Groups, Policies, and RBAC. User roles are documented and administrative and security tasks are logged
6	3.1.6	Use non-privileged accounts or roles when accessing no security functions.	Partially Implemented	Verify only authorized users have access to administrative functions and only use a	On-Premise Active Directory and Group Policy should used for user Authentication,
7	3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Partially Implemented	Verify users	
8	3.1.8	Limit unsuccessful logon attempts.	Not Implemented	This is ODP (Or an	
9	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Not Implemented	Configure log specific bar standard ban	
10	3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity	Not Implemented		
11	3.1.11	Terminate (automatically) a user session after a defined condition.	Not Implemented	Verify or co	
12	3.1.12	Monitor and control remote access sessions	Not Implemented		



Compliance Framework Forecast: CMMCv2

None : 97

Implemented : 7

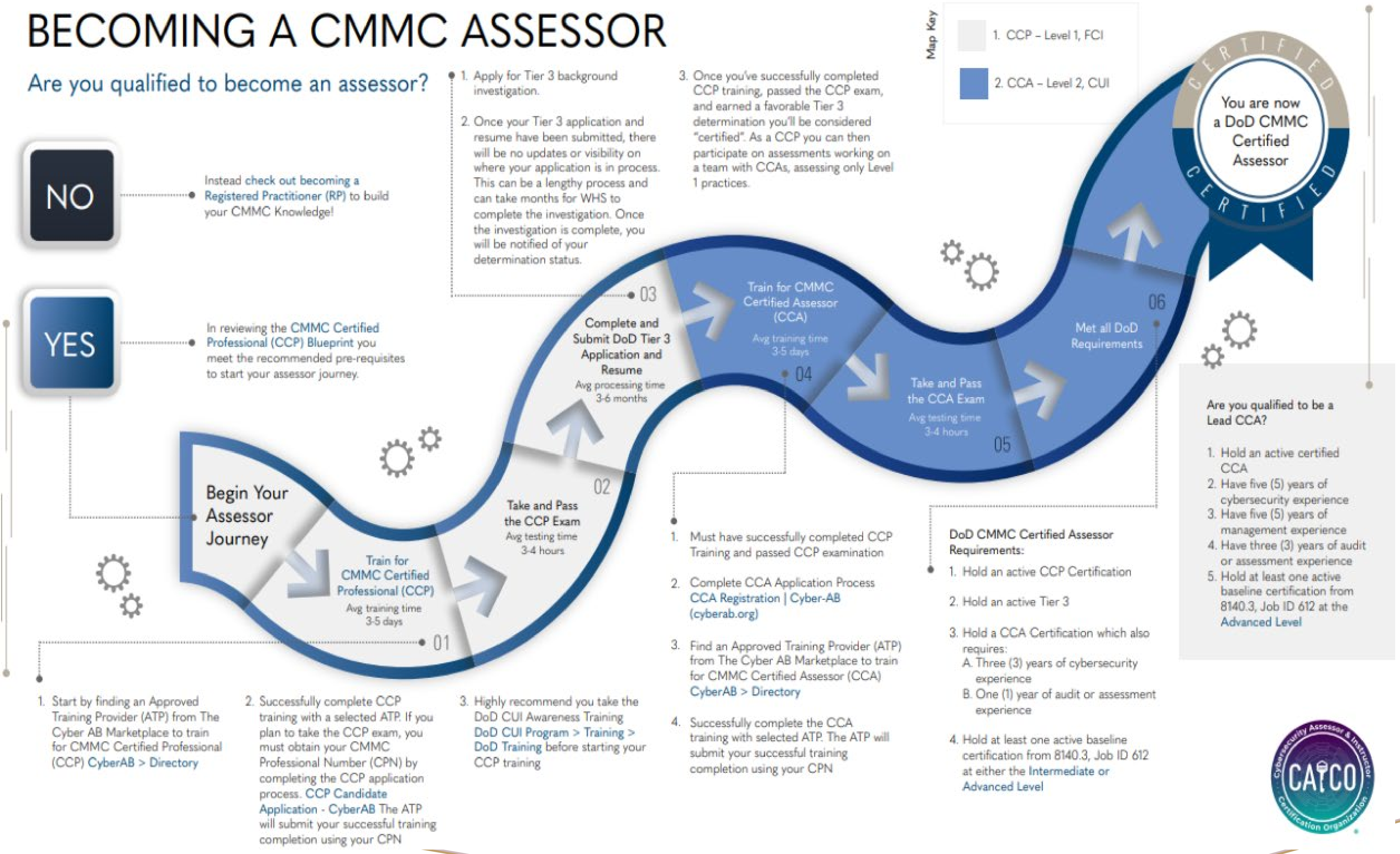
Partially Implemented : 0

Planned : 0

Alternative Implementation : 0

Not Applicable : 0

3RD PARTY ASSESSMENT – C3PAO



BECOMING A CMMC ASSESSOR

Are you qualified to become an assessor?

NO

Instead check out becoming a Registered Practitioner (RP) to build your CMMC Knowledge!

YES

In reviewing the CMMC Certified Professional (CCP) Blueprint you meet the recommended pre-requisites to start your assessor journey.

Map Key

⬜	1. CCP – Level 1, FCI
🟦	2. CCA – Level 2, CUI

Begin Your Assessor Journey
01
Train for CMMC Certified Professional (CCP)
Avg training time 3-5 days
02
Take and Pass the CCP Exam
Avg testing time 3-4 hours
03
Complete and Submit DoD Tier 3 Application and Resume
Avg processing time 3-6 months
Train for CMMC Certified Assessor (CCA)
Avg training time 3-5 days
04
Take and Pass the CCA Exam
Avg testing time 3-4 hours
05
Met all DoD Requirements
06
CERTIFIED
You are now a DoD CMMC Certified Assessor
CERTIFIED

1. Start by finding an Approved Training Provider (ATP) from The Cyber AB Marketplace to train for CMMC Certified Professional (CCP) CyberAB > Directory

2. Successfully complete CCP training with a selected ATP. If you plan to take the CCP exam, you must obtain your CMMC Professional Number (CPN) by completing the CCP application process. CCP Candidate Application - CyberAB The ATP will submit your successful training completion using your CPN

3. Highly recommend you take the DoD CUI Awareness Training DoD CUI Program > Training > DoD Training before starting your CCP training

1. Apply for Tier 3 background investigation.

2. Once your Tier 3 application and resume have been submitted, there will be no updates or visibility on where your application is in process. This can be a lengthy process and can take months for WHS to complete the investigation. Once the investigation is complete, you will be notified of your determination status.

3. Once you've successfully completed CCP training, passed the CCP exam, and earned a favorable Tier 3 determination you'll be considered "certified". As a CCP you can then participate on assessments working on a team with CCAs, assessing only Level 1 practices.

1. Must have successfully completed CCP Training and passed CCP examination

2. Complete CCA Application Process CCA Registration | Cyber-AB (cyberab.org)

3. Find an Approved Training Provider (ATP) from The Cyber AB Marketplace to train for CMMC Certified Assessor (CCA) CyberAB > Directory

4. Successfully complete the CCA training with selected ATP. The ATP will submit your successful training completion using your CPN

DoD CMMC Certified Assessor Requirements:

1. Hold an active CCP Certification

2. Hold an active Tier 3

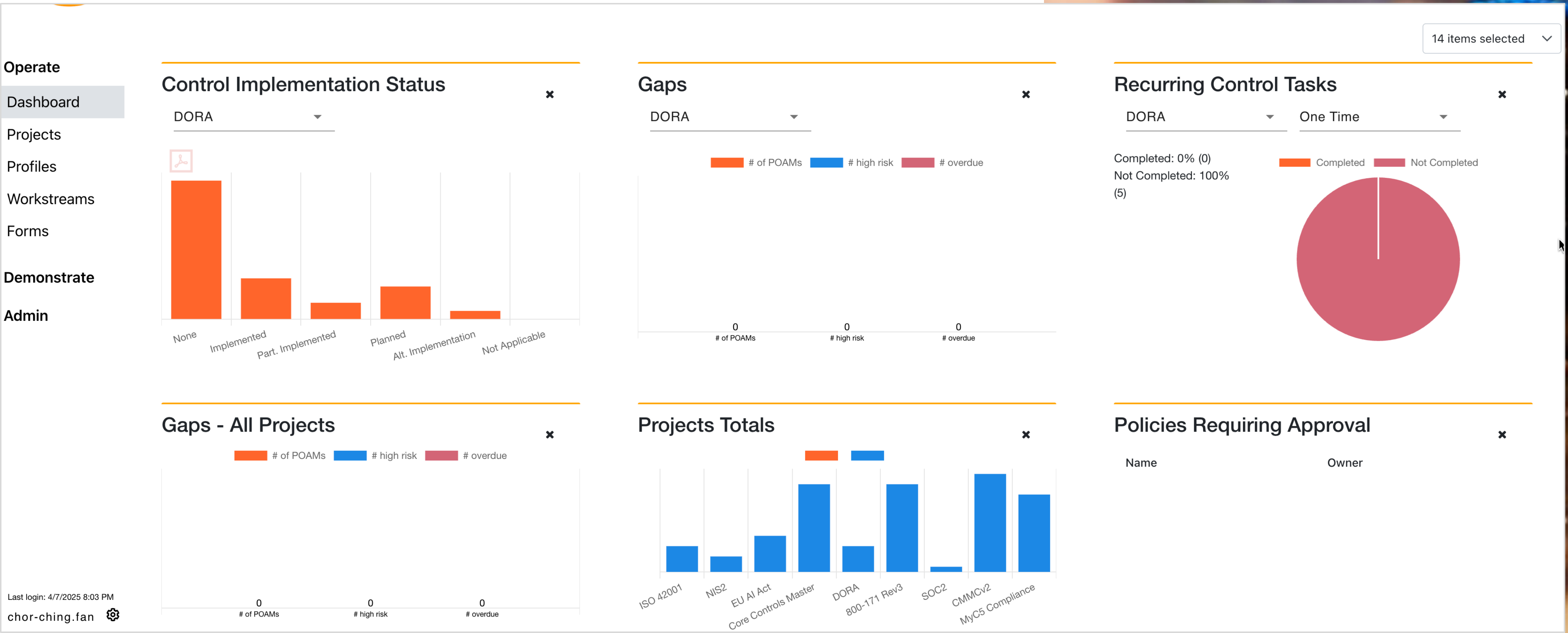
3. Hold a CCA Certification which also requires:
   A. Three (3) years of cybersecurity experience
   B. One (1) year of audit or assessment experience

4. Hold at least one active baseline certification from 8140.3, Job ID 612 at either the Intermediate or Advanced Level

Are you qualified to be a Lead CCA?

1. Hold an active certified CCA
2. Have five (5) years of cybersecurity experience
3. Have five (5) years of management experience
4. Have three (3) years of audit or assessment experience
5. Hold at least one active baseline certification from 8140.3, Job ID 612 at the Advanced Level

CONTINUOUS COMPLIANCE + REAL-TIME VISIBILITY



14 items selected

Operate

Dashboard

Projects

Profiles

Workstreams

Forms

Demonstrate

Admin

Last login: 4/7/2025 8:03 PM

chor-ching.fan

Control Implementation Status

DORA

Gaps

DORA

Recurring Control Tasks

DORA | One Time

Completed: 0% (0)
Not Completed: 100% (5)

Gaps - All Projects

Projects Totals

Policies Requiring Approval

Name	Owner

Level 2 Requires C3PAO every 3 years with yearly audits updated in SPRS

PRACTICAL CONSIDERATIONS FOR DOD CONTRACTORS

BEST PRACTICES

- Prioritize cost-effective automation for assessments and mapping. (Source: https://dodcio.defense.gov/Portals/0/Documents/CMMC/CMMC-FAQs.pdf)
- Utilize free DoD resources like CMMC Academy and guides. (Source: https://dodcio.defense.gov/Portals/0/Documents/CMMC/CMMC-FAQs.pdf)
- Start now: Compliance mandatory for specified contracts **post-Nov 10, 2025**; attend upcoming events like CS5 East Conference (Oct 16-17, 2025) for ecosystem updates. (Source: https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of)

REVIEW OF COMPLIANCE STEPS

	Strategy & Program Management	Assessment & Gap Analysis	Remediation & Documentation	3rd Party Assessment	Monitoring & Reporting
Manual	1 month	1.5 months	13 months	3 months	Continuous
Automated	2 weeks	2 weeks	6 months	1 month	
	50% Savings	66% Savings	54% Faster	25% Faster	50% Savings

DOCUMENT, DOCUMENT, DOCUMENT!

- SSP NIST-800-171 v1.1
- AcceptableUsePolicyv1.0
- Access Control Policy
- Auditing and Accountability Policy
- Configuration Management Policy
- Contingency Planning Policy
- Cyber Incident Response Standard
- Identification and Authentication Policy
- Incident Response Policy
- Maintenance Policy
- Media Protection Policy
- Security Awareness and Training Policy
- Security Assessment and Authorization Policy
- System and Information Integrity Policy
- System and Communications Protection Policy
- Risk Assessment Policy
- Personnel Security Policy
- Physical and Environmental Protection Policy
- Personnel Security Policy
- NIST 800-171 Controls Tracking Spreadsheet 2024
- AccessControlandDataflowPlanv1.0
- Configuration Change Request Tracking Form
- AuditLogPlanv1.0
- ConfigurationManagementPlanv1.0
- IdentificationandAuthenticationPlanv1.0
- Incident Response Tracking Form
- Incident ResponseReportv1.0
- IncidentRepsonsePlanv1.0
- MaintenancePlanv1.0
- Security Assessment
- Risk Management and ContinuousMonitoringPlanv1.0
- SecurityAwarenessTrainingPlanv1.0
- POAM List
- Risk Assessment Report
- SP800-171AssessmentSpreadsheet

CASE STUDY – 50 EMPLOYEE COMPANY

TRADITIONAL MANUAL ASSESSMENT

- Audit required interviews and manual inputting of system, personnel, and CCI Generation.
- Audit to POAM: 3-4 months
- Remediation & upgrades: 8-13 months
- C3PAO Certification: 3 months
- **Total 1.5 years**
- Audit Cost: ~ $60K

SEMI-AUTOMATED ASSESSMENT

- Automated Scanning and system Mapping augments personnel and physical security mapping.
- Audit to POAM: 1 month
- Remediation & Upgrades: 6 months
- C3PAO Certification: 1 month
- **Total 8 Months**
- Audit + Continuous Compliance ~ $30K

REMEDIATION COST VARY WIDELY FROM $10K'S TO $100K

LATEST NEWS

Latest News for DoD Contractors (as of September 16, 2025)

DFARS Final Rule Published and Effective Soon: The Department of Defense released the final DFARS rule on September 10, 2025, implementing CMMC 2.0 requirements in contracts; it becomes effective ***November 10, 2025***, starting Phase 1 with self-assessments for Levels 1 and some Level 2.

Certification Required Before Awards: Contractors must have a "current" CMMC certification or self-assessment in SPRS before contract award or option exercise for deals involving FCI or CUI; no more "win now, certify later.“

POA&Ms and Affirmations Clarified: Plans of Action and Milestones (POA&Ms) are allowed for Levels 2 and 3 (close within 180 days for conditional status); annual affirmations by a senior official are mandatory, with no lapse notifications needed.

Subcontractor Flow down and Small Business Impact: Prime contractors must ensure subs meet the same CMMC levels for FCI/CUI handling; the rule affects about 229,818 small entities over time, with cost estimates for assessments.

THANK YOU

Schedule a free 1-hour consultation today

Contact Information

Josh Hammer

352-467-9699

jhammer@hvfsusa.com

www.hvfssua.com